Title (en)

CRYPTOGRAPHIC MEMORY ATTESTATION

Title (de)

KRYPTOGRAFISCHE SPEICHERATTESTIERUNG

Title (fr)

ATTESTATION DE MÉMOIRE CRYPTOGRAPHIQUE

Publication

EP 3761201 A1 20210106 (EN)

Application

EP 19184108 A 20190703

Priority

EP 19184108 A 20190703

Abstract (en)

According to an example aspect of the present invention, there is provided an apparatus comprising a random access memory device, at least one processing core coupled via a first interface with the random access memory device, and a secure hardware element, comprising hash function circuitry, and coupled directly via a second interface with the random access memory device, the secure hardware element configured to obtain as input data from a memory space of the random access memory device, to produce as output a hash value of the input, and to cryptographically sign the hash value using a physically unclonable function value of the apparatus.

IPC 8 full level

G06F 21/57 (2013.01); **H04L 9/08** (2006.01)

CPC (source: CN EP US)

B60T 17/228 (2013.01 - US); **G06F 21/46** (2013.01 - CN); **G06F 21/57** (2013.01 - EP US); **G06F 21/64** (2013.01 - US); **G06F 21/72** (2013.01 - US); **G06F 21/78** (2013.01 - CN US); **H04L 9/002** (2013.01 - US); **H04L 9/0643** (2013.01 - EP US); **H04L 9/0866** (2013.01 - EP); **H04L 9/0877** (2013.01 - EP); **H04L 9/3006** (2013.01 - US); **H04L 9/3278** (2013.01 - US)

Citation (search report)

- [Y] WO 2009055147 A1 20090430 - MICROSOFT CORP [US]
- [Y] US 2018309578 A1 20181025 - FARRELL BRIAN J [US], et al
- [Y] US 2013254636 A1 20130926 - KIRKPATRICK MICHAEL S [US], et al
- [Y] US 8848905 B1 20140930 - HAMLET JASON R [US], et al

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

EP 3761201 A1 20210106; CN 112182668 A 20210105; US 2021004496 A1 20210107

DOCDB simple family (application)

EP 19184108 A 20190703; CN 202010624979 A 20200702; US 202016916962 A 20200630